UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case Nos. 5:12-cr-37, 5:12-cr-44,
	)	5:12-cr-97
DEREK THOMAS, DOUGLAS NEALE, and STEPHAN LEIKERT	)	
	)	

OPINION AND ORDER DENYING DEFENDANTS' MOTIONS TO SUPPRESS
Defendant Thomas (Docs. 47, 83 & 84)
Defendant Neale (Docs. 24 & 65)
Defendant Leikert (Docs. 22 & 46)

This matter came before the court for an evidentiary hearing on April 17 and July 30-31, 2013 on the motions to suppress filed by Defendants Derek Thomas, Douglas Neale, and Stephan Leikert which were consolidated for the purposes of the court's hearing. The parties' filing of post-hearing memoranda was completed on September 25, 2013.

The government is represented by Assistant U.S. Attorney Nancy J. Creswell in the *Thomas* case; by Assistant U.S. Attorney Timothy C. Doherty, Jr. in the *Neale* case; and by Assistant U.S. Attorney Christina E. Nolan in the *Leikert* case. Defendant Thomas is represented by Elizabeth D. Mann, Esq. Defendant Neale is represented by Assistant Federal Public Defender David L. McColgin. Defendant Leikert is represented by Chandler W. Matson, Esq. and William W. Cobb, Esq.

Each of the Defendants was charged by indictment with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) after law enforcement executed search warrants at their respective residences and seized evidence from a computer or computers found therein. Defendants seek suppression of all evidence derived from the search, arguing that law enforcement's use of automated software constituted a

warrantless search of the private areas of their respective computers in violation of the Fourth Amendment.

In the alternative, Defendants argue that the search warrants in their cases lacked probable cause, and contained false and misleading statements and omissions that intentionally or recklessly misled the magistrate judge who issued the search warrants. Defendants either collectively or individually assert that the search warrant affidavits were false and misleading because they allegedly: (1) failed to adequately disclose and describe law enforcement's use of automated software and a third-party database; (2) failed to disclose the automated software's alleged ability to access incomplete, deleted, and corrupted files, as well as files that had not been made available for sharing; (3) failed to advise of the alleged inadequacy of the testing of the automated software; (4) falsely represented the reliability of hash values to identify a file's contents; (5) falsely stated that an MD4 hash value could be "converted" to a SHA1 value; (6) falsely suggested there was a manual "undercover" investigation; (7) failed to accurately and adequately describe whether and how law enforcement verified the contents of the suspected files; and (8) noted that Defendants allegedly "shared" certain files of child pornography when the files were only allegedly "offered to be shared."

The government opposes the motions, contending that the automated software did not and cannot access "private" files not made available for sharing. Accordingly, it asserts no warrantless searches occurred. The government further contends that the use of automated software was fully disclosed in the search warrant affidavits, the search warrants are supported by probable cause, and the search warrant affidavits contain no intentional or reckless material misstatements of fact or omissions.

I. Findings of Fact.

In approximately December 2011, federal and state law enforcement in Vermont commenced an investigation, known as "Operation Greenwave," into potential child pornography crimes using peer-to-peer file sharing software. Each of the search warrants at issue in this case was part of Operation Greenwave.

A. Peer-to-Peer File Sharing.

Peer-to-peer file sharing is a popular means of obtaining and sharing files free of charge directly from other computer users who are connected to the Internet and who are also using peer-to-peer file sharing software. Peer-to-peer file sharing software is publicly available for download free of charge from the Internet and operates on a particular network which dictates to some extent how the file sharing will occur. Gnutella and eDonkey are two popular networks on which peer-to-peer file sharing takes place.

Generally, the source code for peer-to-peer file sharing software is "open," meaning that, to a certain extent, it may be modified by users. However, although users may make some modifications to the source code, the software must still adhere to a common protocol or language in order for it to communicate with other computers and allow file sharing to take place. There are numerous types of peer-to-peer file sharing programs and numerous versions of each particular type of program.

Once peer-to-peer file sharing software has been downloaded and installed by the user, the user may interface directly with other computers using the same file sharing software and browse and obtain files that have been made available for sharing. The file sharing software does not permit a user to access files that are not available for sharing. However, a user may download a version of the software which contains default settings that make certain files available for sharing without the user's affirmative designation of the files as shared files. In addition, file sharing programs often include a default setting which allows them to operate anytime a computer is on and connected to the Internet even if the user has not sought to reactivate the file sharing program. File sharing programs may resume an interrupted download if the file sharing program is reactivated, even if the user has not affirmatively requested that the download resume.

File sharing occurs when one computer, identified by an Internet Protocol ("IP") address, initiates a search for a responsive file by indicating the term or terms that it seeks to find in the file's name. This is called a "query" and consists of key words such as "child," "pornography," or "child pornography." Law enforcement has identified a

number of search terms commonly associated with child pornography. Other computers that are using the same file sharing software and connected to the Internet at the time will respond to the query with a "query hit message." A query hit message identifies the file or files available for sharing which have a word in the file name that matches the search word in the query. The query hit message will also contain additional information such as the IP addresses of the computers offering to share responsive files. Often multiple computers will respond to a single query.

After a query hit message is received, the computer user requesting the file must affirmatively select it for download, generally by double clicking on the file's name. It is possible and even probable that the download will occur from multiple computers at the same time all of which have responded with a query hit message and are simultaneously sending the file for download to the computer requesting it. This permits a more rapid downloading process. A person seeking to download a file may often preview a portion of the file before downloading it, however, some peer-to-peer file sharing software programs do not allow the user to view the file until the download is complete. Incomplete files are generally not available for download unless the computer user responding to a query, or the default settings on his or her computer, have made an incomplete file available for sharing.

Peer-to-peer file sharing software also often allows a user to request a "browse host," which is a request to view all of the files that another computer has available for sharing. Both the Gnutella and eDonkey networks have a browse host function built into their protocols. eDonkey, however, relies on actual servers while Gnutella does not. Accordingly, a user of the eDonkey network submits his or her shared files to eDonkey's servers, and the servers respond on behalf of users who are then online and operating eDonkey file sharing software. Both networks use a query-response protocol whereby queries are sent out, responses are received and displayed, and the user then selects the files he or she seeks to download or simply browses the files made available for sharing. It is not uncommon for a user to download all of another user's files available for sharing and then determine at a later time whether to retain those files.

Many peer-to-peer file sharing programs permit the user to disable the file sharing component of the software. In addition, the software may be configured to prohibit the use of the browse host function. However, because the software is open source code, it is not always certain that the peer-to-peer file sharing software will function as intended by the user. If a user's computer is either off or not connected to the Internet, no file sharing will take place.

B. Hash Values.

Peer-to-peer file sharing programs all use hash values to identify files in a manner that is significantly more precise than a file's name. A hash value is a list of characters that act as a digital fingerprint for a file's contents. Hash values have varying degrees of reliability. The network chooses the type of hash value it will use for file sharing purposes. Law enforcement agents investigating peer-to-peer file sharing activity will thus receive responses that reflect the network's chosen type of hash value.

The Secure Hash Algorithm ("SHA1") value consists of thirty-two characters and was developed by the National Security Administration in 1992. It is more reliable than DNA (in that the likelihood of two individuals coincidentally sharing the same DNA is greater than the likelihood that more than one file will have the same SHA1 value) and a collision[1] between two files with identical SHA1 values but with non-identical content has never been shown to exist. The Gnutella network uses the SHA1 value.

The eDonkey Network uses the MD4 hash value, which divides every file into 9.5 kilobytes, assigns a hash value to each part, and then assigns a hash value to the completed file. The component hash values are not stored separately. eMule, which is the most popular peer-to-peer file sharing program on the eDonkey network, uses the MD4 hash value as its unique identifier for files. There is no evidence that an MD4 hash value is inherently unreliable and cannot be used to identify files. To the contrary, it is a substantially more accurate means of identifying a file than the file's name.

[1] In computer forensics terminology, a "collision" is when two non-identical files share the same hash value.

There is no way to "convert" a MD4 hash value into a SHA1 value or vice versa. However, a law enforcement officer may access a database that identifies all of the hash values believed to be associated with a particular file and thereby cross-reference the different types of hash values that have been associated with the file. Software that performs this function is publicly available on the Internet.

C. TLO's Investigative Software Tools.

William Wiltse, a former law enforcement officer, certified computer forensics examiner, and experienced programmer, created or assisted others in the creation of a suite of software programs to automate, expedite, and focus law enforcement's investigation of child exploitation crimes. Through a company called TLO, a data fusion company, Mr. Wiltse and his colleagues offer a suite of software and other products known collectively as the Child Protection System ("CPS") free of charge to licensed law enforcement professionals. TLO has trained law enforcement officers investigating child exploitation crimes in forty-two countries.

Among the products TLO offers are certain products that substitute automation for the computer key strokes and data gathering a law enforcement officer would otherwise perform manually in order to investigate peer-to-peer file sharing software crimes. Rather than sitting at a computer sending out queries and evaluating responses, and then attempting to narrow search results in a relevant manner, a law enforcement officer may use CPS products to automate this process.

CPS is a web interface or portal which permits a user to access CPS's suite of tools. In order to use CPS products, law enforcement must attend and successfully complete an approximately three day training course. In the course, law enforcement officers are instructed regarding how to search for child pornography with peer-to-peer file sharing software using both a manual method and a CPS tool known as Peer Spectre which automates the query-response function. Law enforcement is then instructed regarding how to compare the results. If a law enforcement officer successfully completes the course, TLO issues the law enforcement officer a license to access CPS's suite of tools in his or her jurisdiction.

None of CPS's products have any ability to infiltrate a user's computer with child pornography because TLO does not possess, contain, or warehouse any actual images of child pornography or suspected child pornography. Moreover, because CPS software is based upon query-response software, the only information it gleans is information a user's computer has made available for sharing. As a further limitation, CPS tools gather only file names, hash values, and other data; they have no ability to access the images or files themselves. A law enforcement officer must therefore follow-up on the leads generated by CPS tools. He or she may decide to attempt a direct download from a particular IP address or consult his or her own agency's database or another available database of known child pornography to determine whether a file which corresponds to a particular hash value appears to contain suspected child pornography.

Peer Spectre is part of CPS's suite of tools and is a software application that focuses on the Gnutella file sharing network. It operates on a law enforcement officer's own computer and automates the process of sending out queries for files by using terms known to be associated with child pornography. If a user is online and has activated peer-to-peer file sharing software, his or her computer will respond to Peer Spectre's query with a query hit message, indicating that the computer has offered to share a responsive file or files. The query hit message generally includes the full file name, the file size, the hash value which identifies the file, the Globally Unique Identifier ("GUID") which is akin to a software serial number, the IP address of the computer offering to share the file, and the port it is using. Peer Spectre then analyzes the information received and sends a report of that information to the law enforcement officer, who may analyze it immediately or at a later time.

Because peer-to-peer file sharing programs operate globally and contain no internal distinction regarding geography, TLO uses publicly available geo-location technology to narrow search results to geographic areas of interest. This allows TLO to identify a country, state, and city for every query hit message. In turn, TLO is able to ensure that only those query hit messages that constitute responses from IP addresses within the law enforcement officer's licensed jurisdiction will be reported back to the

officer. In most cases, there are more identified IP addresses for a particular geographic region than a law enforcement officer can reasonably investigate so the report generated by the automated software assists the officer in prioritizing his or her investigation by identifying the "worst" IP addresses, (in terms of the likelihood that the IP address is offering to share child pornography). In contrast, using a manual method, a law enforcement officer may receive query hit messages from computers in other states or other countries and thus must manually narrow those responses by determining whether the IP address reflects an Internet provider in his or her jurisdiction.

TLO developed Lime Crawler and Lime Scanner to run on TLO's own servers. Lime Crawler and Lime Scanner are one piece of software divided into two parts to automate the process of investigating the use of Limewire peer-to-peer file sharing programs. Lime Scanner sends out the query messages and Lime Crawler attempts to make a direct connection with the IP address by sending a browse host request, asking to see the other files that a particular IP address has made available for sharing. These programs operate on both the eDonkey and the Gnutella networks.

Nordic Mule is a software program, originally developed by law enforcement agents in Norway, that TLO has modified for use in a manner similar to Peer Spectre but which operates on the eDonkey network. Nordic Mule thus uses the MD4 hash value used by the eDonkey network. Like Lime Scanner and Lime Crawler, Nordic Mule is only used internally at TLO and resides on TLO's servers. It has the ability to automate the browse host function and submit responses to TLO's servers, which then generate a report of the results for law enforcement.

TLO's Media Library allows law enforcement to research whether a particular file has previously been determined by law enforcement to contain potential child pornography. The Media Library database contains over 330,000 file entries and resides on TLO's servers. It, however, contains only hash values, file names, and file information. It contains no actual files or images of child pornography. Media Library does not verify the accuracy of the characterization of its files as suspected child pornography beyond the initial process by which a particular file is submitted to its

database. It thus does not and cannot make the legal determination as to whether a particular file depicts child pornography as the definition of "child pornography" varies from jurisdiction to jurisdiction.

For each file, Media Library contains all known hash values associated with it including SHA1, Tiger tree, and MD4 hash values. In this respect, if a file is identified, a law enforcement officer can gain access to each type of hash value that has been associated with it. Other publicly available software programs offer this same functionality. A law enforcement officer may access Media Library even if he or she chooses not to use Peer Spectre or any of TLO's other products.

D. Testing of CPS Tools.

In order to test Peer Spectre, programmers used a program called a "packet capture" that allows a programmer to effectively eavesdrop on the network transmissions from that program out to the Internet. They then determined whether they could reliably connect and maintain a connection within a closed network environment to validate whether the queries were generating appropriate query hit messages. TLO tested Lime Scanner and Lime Crawler by comparing their performance with Peer Spectre, to determine whether both types of programs were generating the same leads regarding IP addresses. TLO concluded that no further testing was necessary as those products are based upon an existing source code which is the protocol for the networks on which they operate. Because Nordic Mule was built on the eMule source code by investigators in Norway, TLO did not test it further.

Mr. Wiltse opined that the reliability of CPS query-response software products has been established by marketplace acceptance. He explained that each of these programs uses the same protocol as the networks on which they are based, which offer popular file sharing programs that would not be used if they did not function as intended.

Defendants challenge Mr. Wiltse's opinion that CPS products are reliable. They contend that TLO must test and establish a known error rate for CPS products before they may be used to support a finding of probable cause. Defendants do not, however, suggest a manner in which such an error rate could or should be established. Since CPS's query-

response software programs are based upon the same protocol used by the file sharing network they investigate, it is not clear what, if any, adjustments could be made to them to render them more "reliable." There is no evidence that CPS products report false or misleading information. Instead, they are evidence-gathering tools that merely obtain, report, and categorize information regarding files that are available for sharing from a particular IP address. A law enforcement officer must then take further steps to determine whether the information received supports a conclusion that there is probable cause to believe that evidence of child pornography will be found at a particular physical address.

E. Affidavits in Support of Probable Cause.

In each of these cases, law enforcement used a common template for the affidavits in support of probable cause which were used to obtain search warrants for Defendants' respective residences. The template was a collaborative drafting effort by a number of law enforcement officers and borrowed heavily from a search warrant affidavit that had been used to secure a Vermont state court search warrant. The template also reflected information obtained from an ICE Agent in New Hampshire who had drafted affidavits for child pornography search warrants in other cases. In each of Defendant's cases, law enforcement did not attempt a direct download or a browse host from a target IP address. Instead, law enforcement relied upon "historical" information to establish probable cause. Each search warrant affidavit recites the investigative steps that were taken thereafter to determine the residence with which a target IP address was associated.

Detective Corporal Gerry Eno, identified in each of the search warrant affidavits as a source of information, is the coordinator of an undercover operations unit that investigates child exploitation crimes. All proactive investigations conducted by Vermont's Internet Crimes Against Children Task Force ("ICAC") fall within his undercover unit which has been performing peer-to-peer file sharing investigations since approximately 2007. For this reason, Detective Eno refers to peer-to-peer file sharing investigations as "undercover investigations."

ICAC maintains a library of files that contain images and videos of child pornography and their associated hash values. Law enforcement officers may access ICAC's library or an officer's own agency's library to attempt to determine whether a particular file contains potential child pornography by comparing the hash values of the files.

Detective Eno has completed TLO's training course and is licensed to use CPS products in his jurisdiction. In the course of his training, he and his training class compared manual search results with those generated by TLO's automated software, and no discrepancies in the search results were noted. In these cases, he chose a historical investigation approach using automated software in order to maximize limited investigative resources and to eliminate the uncertainty of trying to predict when a particular IP address was online.

Prior to submitting the search warrant applications to the magistrate judge, law enforcement submitted them to an Assistant United States Attorney for review and approval. The law enforcement officers who signed the search warrant affidavits credibly testified that they believed the contents of their affidavits were true and correct to the best of their knowledge when they submitted them to the magistrate judge. They further credibly testified that they maintain that same belief notwithstanding Defendants' challenges. None of the affiants is an expert in computer forensics or claims such status in his or her affidavit.

Each search warrant affidavit is approximately thirty pages in length with several pages of attachments. Each contains introductory paragraphs identifying the affiant, the place to be searched, and the items to be seized. Each affidavit states that the information contained therein is based on an investigation conducted by the affiant and other law enforcement agents and states further that: "This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts that I believe to be necessary to establish probable cause for issuance of a search warrant for the Subject Premises." Ex. 7 at ¶ 5; Ex. 8 at ¶ 5; Ex. 9 at ¶ 5.

The affidavits cite the criminal statutes alleged to have been violated followed by a lengthy list of definitions of relevant terms. Thereafter, the affidavits contain approximately ten paragraphs under the heading "Background on Computers and Child Pornography" which explain, in some detail, how child pornography crimes are committed using computers and how evidence of child pornography may be detected on a computer. The affidavits disclose the use of third party software to identify the IP address of a target computer and to monitor and log Internet and local network traffic from that IP address.

Each search warrant contains an additional section entitled "Specifics of Search and Seizure of Computer Systems," which explains how data is extracted from a seized computer and the technology, resources, and time generally needed for this process.

Defendants' challenges in these cases are primarily directed to a section of the search warrant affidavits entitled "Background of Investigation." Defendants claim that this section insufficiently discloses law enforcement's use of automated software from a third party source; overstates the reliability of hash values; erroneously characterizes the investigation as "undercover"; and omits facts that would have allowed the magistrate judge to evaluate the automated software's reliability. The challenged section is therefore set forth in its entirety with the particular language at issue in bold:

> A growing phenomenon on the Internet is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. The Gnutella and eDonkey networks are two of the most popular file sharing networks today. A number of software applications support file sharing on the Gnutella and eDonkey networks. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are of interest and currently being shared on the network. Client programs participating in the Gnutella or eDonkey networks, such as Limewire, set up their searches by keywords. The results of a keyword search are displayed to the user. The user then selects the file(s) from the results for download. The download of

a file is achieved through a direct connection between the computer requesting the file and one or more computers containing the file.

For example, a person interested in obtaining child pornographic images would open the Gnutella or eDonkey P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed the file(s) he or she wants to download. The file is downloaded directly from the computer(s) hosting the file. The downloaded file is stored in the area previously designated by the user. During the installation process the client program can select a pre-determined folder for the downloaded files to be placed in. This folder is generally the "shared" folder. The user can change the download location at any time, during the installation process or thereafter. The downloaded file will remain until moved or deleted. Users attempting to trade files on a P2P file sharing network can place files from their own computer in a shared file directory. The P2P software installed on the computer calculates the hash value (described below) for each shared file and provides that information to other users on the P2P network.

One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a Limewire user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a Limewire user downloading an image file receives the entire image from one computer. Another feature of P2P file-sharing networks is the browsing of (receive a list of) all the files a particular computer is sharing. The P2P program allows users to see all of the files that an individual user is sharing. **If the sharing computer is in the process of downloading file(s) (incomplete files), these files do not appear in the list. Only those that are completely downloaded and being shared will be displayed in this list.** A user may also add other files into this shared file list which were not downloaded by this client.

The Gnutella Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the fingerprinting of files. Once you check a file with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The Secure Hash Algorithm was developed by the Institute of Standards and Technology and the National

Security Agency. The federal government has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. **The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.** When a user browses or views the entire list of files being shared by a computer system running Limewire (or any other Gnutella Client), the SHA1 hash value is visible and can be logged. One of the P2P networks investigated in this operation uses the SHA1 digital signature to verify the unique identity of individual files. A person is able to compare the SHA1 hash values of files being shared on the network to previously identified SHA1 hash values of any file, including child pornography files.

The eDonkey network is a decentralized, peer-to-peer file sharing network best suited to share big files among users, and to provide long term availability of files. Like most sharing networks, it is decentralized, as there is not any central hub for the network; also, files are not stored on a central server but are exchanged directly between users based on the peer-to-peer principle.

eDonkey uses a different hash algorithm than the Gnutella network to identify files, namely, the MD4 hash algorithm. Files located in a user's shared directory are processed by the client software, and an MD4 hash value is computed for each file in the user's shared directory. **MD4 verifies the identity of a digital file.**

The eDonkey network uses MD4 hash values to improve network efficiency. As with the Gnutella network, users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. **The network uses MD4 hash values to ensure exact copies of the same file are used during this process.**

A person is able to compare the MD4 hash values of files being shared on the network to previously identified MD4 hash values of any file, including child pornography. Using a publicly available eDonkey client program, a user can select the MD4 hash value of a known file and attempt to receive it. Once a specific file is identified, the download process can be initiated. Once initiated, a user is presented with a list of users or IP addresses that have recently been identified as download candidates for that file. This allows for the detection and investigation of computers involved in

possession, receiving and/or distributing files of previously identified child pornography.

When law enforcement identifies child pornography being shared on the eDonkey network, it can hash the file using the SHA1 digital algorithm and determine its SHA1 value. Once the hash value is converted to SHA1, law enforcement can search for the file on the Gnutella network. For the purposes of this investigation, law enforcement needs to convert the eDonkey hash value to SHA1 because it is able to search for files by hash value only on the Gnutella network.

A P2P file transfer is assisted by reference to an IP address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

The computer running the file sharing application has an IP address assigned to it while it is on the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to determine the Internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the Internet service provider. By examining a list of IP addresses sharing files, law enforcement can locate computers that are reported to be in Vermont. **By comparing the SHA1 digital signatures to files that are shared by the Vermont-based computers, investigators know that these computers are sharing files known to depict the sexual exploitation of children on the P2P network.**

As part of this operation, Detective Corporal Gerry Eno of the Vermont Internet Crimes Against Children (ICAC) Task Force and the South Burlington Police Department confirmed that each [SHA1] value of interest to the investigation actually represents an image or movie that depicts child pornography. **Detective Corporal Eno did this by viewing an image or movie with the same SHA1 signature as the shared file. Detective Corporal Eno located the image or movie in the VT ICAC database, or otherwise obtained a copy from another source (or multiple sources) on the P2P network.**

During this investigation, law enforcement used software that automates the process of searching for computers in Vermont that are suspected of sharing images or videos depicting child pornography on

> **P2P networks. This software is designed to replace the searches that were previously done manually by law enforcement and the public. The software reports information that is discoverable by the general public using publicly available P2P software. Investigators who have access to this software physically activate the software in order to begin the search process which then automatically reads the publicly available advertisements from computers that are sharing files depicting child pornography. The software reads the offers to participate in the sharing of child pornography and logs the IP address, time, date, SHA1 values, and [file name] of each individual computer in the same way every time. Law enforcement has validated this software by running identical search terms through the manual method described above and have confirmed that the software performs in the same way.**

Ex. 7 at ¶¶ 21-33; Ex. 8 at ¶¶ 21-33; Ex. 9 at ¶¶ 21-33 (emphasis supplied).

Defendants further challenge a portion of the search warrant affidavits in a section entitled "Probable Cause" which explains how in December of 2011, Detective Corporal Eno "was conducting undercover operations" on an identified file sharing network and noted that an identified IP address had previously shared files identified by their hash values as containing child pornography. Ex. 7 at ¶ 34; Ex. 8 at ¶ 34, Ex. 9 at ¶ 34. The affidavits note that Detective Eno "determined" the SHA1 hash values for certain of these files "and was able to view them, either by searching for and downloading them on the Gnutella network or by locating them within a library of files and associated SHA1 hash values maintained by the Vermont Internet Crimes Against Children Task Force." Ex. 7 at ¶ 35; Ex. 8 at ¶ 34; Ex. 9 at ¶ 34.

Each of the search warrant affidavits thereafter contains a description of the alleged child pornography offered to be shared, information regarding the IP address, and law enforcement's efforts to identify a specific residence associated with the IP address.

F. Computer Forensics Expert Tami Loehrs.

Tami Loehrs testified as an expert in computer forensics on behalf of Defendants Neale and Leikert. She performed no work on behalf of Defendant Thomas. The government did not challenge her qualifications to testify. She is both a certified

computer forensic examiner and a private investigator. She has testified as a computer forensics expert approximately seventy-five times.

Ms. Loehrs was asked to prepare an expert report in the *Neale* case which was admitted as Exhibit B. Her declaration in the *Neale* case dated December 20, 2012 was admitted as Exhibit C. Ms. Loehrs was not asked to prepare an expert report in the *Leikert* case, although she submitted a declaration which was admitted into evidence as Exhibit 16.

Ms. Loehrs's declarations filed in *Neale* and *Leikert* are misleading in several respects. For example, in each of them, Ms. Loehrs stated that she needed to test Peer Spectre software because "this is the very same automated software used by law enforcement in numerous cases throughout the country in which I have been involved as a defense expert. These cases have brought to light serious concerns with regard to the . . . software used by law enforcement during undercover P2P investigations[.]" Ex. C at ¶ 10; Ex. 16 at ¶ 11. She further testified that peer-to-peer software is not validated, tested, or reliable, noting specifically that "Peer Spectre in any searching does rely on the reliability of these networks that we're searching. And these networks are horribly unreliable." (Tr. 7/30/13 at 73.) She conceded that there is no available protocol for testing peer-to-peer file sharing software. She cites no court and no learned treatise or peer-reviewed research that has endorsed her concerns. She also cited no evidence that any court has granted a motion to suppress based on her testimony or has expressed "serious concerns" with law enforcement's use of Peer Spectre or with any other CPS products.

As a preface to a list of twenty-five cases identified in her declarations, Ms. Loehrs states: "I have also learned through hundreds of forensic examinations on cases involving undercover P2P investigations and allegations of child pornography, that files are being identified by law enforcement's automated software as containing child pornography when, in fact, they do not." Ex. C at ¶ 19; Ex. 16 at ¶ 20. However, none of the cases listed in Ms. Loehrs's declarations appeared to have resulted in a judicial finding to that effect. To the extent Ms. Loehrs relies on her findings in the *Neale* and

Leikert cases for this statement, she concedes that there are additional facts, not disclosed in her declarations or report, which may explain her findings.

In her declaration filed in the *Neale* case, Ms. Loehrs stated that she did not find the files identified in the *Neale* search warrant affidavit on Defendant Neale's computer when she examined it. She further asserts that the government's forensic examination of the evidence did not reveal those files on Defendant Neale's computer. However, on cross-examination, she acknowledged that other evidence of possession of child pornography was found by the government on Defendant Neale's computer including variations of the file names in the search warrant affidavit (appended with a different number at the end of the file name). This information is not included in either her report or declaration.

Similarly, in *Leikert*, in her declaration Ms. Loehrs noted that the specific images identified in the *Leikert* search warrant application were not later found on Defendant Leikert's computer. She again notes that the government's forensic report reflects the same finding. On cross-examination, however, she acknowledged that Mr. Leikert re-installed the operating system of his computer before the search warrant's execution. In such event, she acknowledges that any pre-existing files would be destroyed. Again, this fact was not disclosed in her declaration.

Ms. Loehrs opined that a SHA1 value is not a reliable indicator of a file's contents and that more than one file may have the same SHA1 value. She later clarified her testimony to acknowledge that she had personally never seen or heard of a SHA1 value colliding, and she acknowledged that two files with the same SHA1 value cannot have different content. (Tr. 7/30/13 at 86, 87.) She asserted a similar opinion with regard to the MD4 hash value, but did not cite to any specific instances of collisions or any research that has found an MD4 hash value cannot reliably be used to identify a file's contents.

Although Ms. Loehrs testified that in order for a person to obtain child pornography files using a peer-to-peer file sharing program, "[t]ypically they have to be selected somehow" (Tr. 7/30/13 at 139), she further testified that for a "number of

reasons," an individual may have a SHA1 value for a child pornography file on his or her computer without having intentionally downloaded the file. (Tr. 7/30/13 at 56.) She explained that "SHA values and files names can be downloaded onto your computer while you're downloading other files that have nothing to do with those. They could get on your computer because of viruses, Trojans, hackers. [A]nyone who has kids at home who used the computer to download stuff they could be getting SHA values and file names on your computer. There's a multitude of ways those can be on there." *Id.* She disagrees with Mr. Wiltse's testimony that a virus cannot be embedded in an image file, although she testified that: "I don't know if I've specifically seen one embedded in an image file myself. [B]ut it, it's absolutely out there. All you have to do is go to the virus protection software and they'll tell you about them. I don't know that I have specifically—I can't recall an instance where I know of a virus embedded in an image file but, yes, it's possible." (Tr. 7/30/13 at 83-84.) At the prompting of defense counsel, Ms. Loehrs then recalled one instance in which she allegedly witnessed a virus embedded in a video file. Here, the court need not decide whether Ms. Loehrs's testimony is credible and sufficiently reliable because there is no evidence before the court that the evidence of alleged child pornography discovered on Defendants' computers was the product of a virus or by any other unintentional means or process. Even if such evidence existed, it may provide a defense to the merits of the case, but it would not preclude a finding of probable cause.

The most troubling aspect of Ms. Loehrs's expert opinions in this case is her reliance on her work in other cases which was either disproved or rejected. For example, she testified that "it is evident from my investigation that Peer Spectre has the ability to identify files that are not publicly available" (Tr. 7/30/13 at 117) and that "[a]ll of my testing, research, communication with other experts in the field that have found the very same thing" support her conclusion that "SHA values and files names that exist in [a computer's] hidden system files regardless of [whether] they are associated with file sharing are being reported as actual shared files when in fact they are not and may have never been." (Tr. 7/30/13 at 61.) From her perspective, "that's the issue, [it] is the

communication between code and code into these hidden files. It's not what the user is seeing in their so-called shared folder." *Id.* She cited an article authored by Joseph Lithwait and Victoria Smith that purportedly states that a computer's fileurns.cache holds the SHA1 value of shared files when in actuality it holds SHA1 values of files that have been deleted. She also "created" a screen shot by manually placing incomplete, empty, and preview files (from both Phex and Limewire) in a shared folder to demonstrate what she has allegedly previously seen in her computer forensics career.

In support of the opinions she offers in *Neale* and *Leikert*, Ms. Loehrs relies heavily on her work in two state court cases. She cites her forensic work in *State of Arizona v. Lemuel Robson*, in which Mr. Robson had his file sharing turned off at the time Peer Spectre identified files available for sharing. In her declaration filed in the *Leikert* case, she queries: "With sharing turned off, nothing on Robson's computer should have been publicly available and the question[] remains, 'how did law enforcement's software identify those files?'" Ex. 16 at ¶ 26. She concludes that Peer Spectre must have identified Mr. Robson's "private" files. However, in cross-examination, Ms. Loehrs conceded that Mr. Robson had a roommate whose computer used the same router and IP address. She initially testified that she did not recall whether the roommate's computer contained the images of suspected child pornography identified in law enforcement's investigation and testified that she did not recall the facts of the *Robson* case. (Tr. 7/30/13 at 124-25.) After reviewing the government's forensic investigation report in *Robson*, Ms. Loehrs conceded that the report indicated that two files of suspected child pornography found by the investigating officer were in fact found on the roommate's computer. (Tr. 7/30/13 at 119-20.) These facts were omitted from her description of her work in the *Robson* case in her declarations filed in this case. Ms. Loehers ultimately agreed that a file must be made available for file sharing either by a user or by the default settings of the user's software program before it will be shared.[2]

[2] Question: "So you admit that just because there is data in a computer in various places, various systems files as you put it, that doesn't mean that it's available for sharing always?"

Ms. Loehrs further relies on what she described as "very formal testing" (Tr. 7/30/13 at 19) she allegedly performed at the request of the court in *State of Arizona v. Robert Dean Moran*, CR2009-114677-001 SE (Maricopa County Superior Court Sept. 11, 2012). Defendants introduced into evidence without objection a report of P2P file sharing testing dated September 28, 2011 that Ms. Loehrs prepared for the *Moran* case, as well as her affidavit submitted to the *Moran* court. In *Moran*, Ms. Loehrs performed testing which she claims revealed that a browse host function can show as available for sharing partial, incomplete, deleted, and corrupt files. She further testified that her testing in *Moran* revealed that "child pornography was actually created in a hidden system folder that the user doesn't have access to," which was a video file with a virus. (Tr. 7/30/13 at 78.)

Ms. Loehrs testified that she has not read the *Moran* court's opinion although it was provided to the attorneys who called her as a witness in this case. The court finds Ms. Loehrs's claim in this respect either incredible or reflective of a lack of concern regarding the reliability of the opinions she is offering under oath. Many of the opinions advanced by Ms. Loehrs in the *Neale* and *Leikert* cases were the same opinions she advanced in *Moran*. The *Moran* court squarely rejected those opinions, finding that "Ms. Loehrs . . . could not explain her own testing methods based on her screenshots she provided" and that, "[o]verall, [Ms. Loehrs] provided testing screen captures to this Court that were inaccurate, incomplete, and thus misleading as they did not fully set forth in detail the testing she asserts . . . supports her contention that there are flaws with the Peer Spectre program." *Moran*, at 9. The *Moran* court further rejected Ms. Loehrs's testimony that "a SHA-1 value or Hash Value of an image was not reliable and thus dangerous for a [d]etective to use as a basis for probable cause" and specifically rejected

---

Ms. Loehrs: "I've never said that that's the case. Only if it's in a file sharing system file that's being read by other file sharing."

Tr. 7/30/13 at 137.

her conclusion that a single source download was required to establish probable cause. *Id.* at 10. As the *Moran* court observed:

> Ms. Loehrs uses her opinion about single source downloads to further support . . . her contention of the lack of probable cause in this case. To that end, Ms. Loehrs testified that a single source download is required to prove that the Defendant was in possession of the child pornography, she however could not tell this Court where she learned this information. Nor could she tell this Court the training or the person from whom she learned this requirement. Ms. Loehrs further failed to provide this Court with any information, be it training materials, case law, or otherwise, that asserts that officers are **required** to perform single source downloads of their investigations.
>
> Once again, Ms. Loehrs has proven inaccurate as all of the officers who testified before this Court, including State's Expert Corporal Erdely, indicated that there is no requirement of officers to perform a single source download of an image.
>
> * * *
>
> Ms. Loehrs testified and swore in her affidavit to this Court, that the Victoria Smith article submitted as evidence articulated the requirement for a single source download. Ms. Loehrs further indicated that the article supported her claims that incomplete, deleted, corrupted and empty files will show in the Peer to Peer network downloads as files available for sharing. Ms. Loehrs['s] contention is that these incomplete files, corrupted files, partial files, would show in the fileurns.cache as available for sharing. The Victoria Smith article clearly states otherwise. In fact, the article is certain that these files would go into the downloads.dat file and not show as available for sharing. Ms. Loehrs ultimately conceded that the sworn statements in her affidavit to this Court about the Victoria Smith article do not support the arguments she claimed.

Id. at 10-11 (internal citations omitted).

In light of the *Moran* court's rejection of Ms. Loehrs's expert opinions, she should not have relied on the *Moran* testing in this case. On balance, Ms. Loehrs provided little, if any, credible or reliable testimony to support her expert opinions in this case. Accordingly, the court does not rely on her opinions in reaching its conclusions.

G. Computer Forensics Expert Laurie Mintzer.

Defendant Thomas called Laurie Mintzer as an expert witness in computer forensics. The government did not challenge her qualifications to testify. Ms. Mintzer performed a forensic examination of Defendant Thomas's computer and determined that

peer-to-peer file sharing software was active on his computer, that FrostWire once existed on his computer, that Shareaza once existed on his computer, and that while eMule downloads were found, there was no reference to them in the computer's program file. She was able to locate one of the files identified in law enforcement's search warrant affidavit on Mr. Thomas's computer, but did not find it in a shared folder. She opined that it was possible that the file was never in a shared folder if law enforcement was sending out a query simultaneously with Defendant Thomas's downloading of the file. (Tr. 7/30/13 at 164.) She further testified that files that are in the midst of being downloaded could be shown as available for sharing even though, in the midst of a download, they are incomplete. However, she conceded that no actual sharing will take place unless the download is complete and the file is made available for sharing. She contends that an actual download of the file and an examination of its contents is a "better way" to validate Peer Spectre. (Tr. 7/30/13 at 174.) She cited no research or authority for this opinion.

Although Ms. Mintzer had never seen a collision with a SHA1 value, she read an article which described how a "Professor Wong, Wong or Wang" showed the "possibility" that "with brute force" a SHA1 hash value could be compromised. (Tr. 7/30/13 at 170, 171.) Ms. Mintzer did not provide a copy of this article to the court, and the court has no other information regarding its existence.

The court accepts Ms. Mintzer's opinion that a computer in the midst of downloading a file may indicate that the file is available for sharing when in fact it is not until the download is complete. The court rejects the remainder of Ms. Mintzer's opinions as unsupported by reliable evidence.

II. Conclusions of Law and Analysis.

Each of the Defendants argues that law enforcement engaged in a warrantless search of the private areas of their respective computers. The court thus considers whether a "search" occurred in terms of the Fourth Amendment and, if so, whether the absence of a warrant rendered that search unconstitutional. If a warrantless search did not occur, Defendants maintain that suppression of the evidence derived from the search warrants remains appropriate because law enforcement intentionally or recklessly misled the magistrate judge by including material misstatements and omissions of fact in the supporting search warrant affidavits which, if corrected, defeat a finding of probable cause.

A. Standard of Review.

"It is well established that the burden of production and persuasion generally rest upon the movant in a suppression hearing." *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980) (internal quotation marks omitted); *see also United States v. Joseph*, 332 F. Supp. 2d 571, 574 (S.D.N.Y. 2004) (same). "The movant can shift the burden of persuasion to the Government and require it to justify its search, however, when the search was conducted without a warrant." *Arboleda*, 633 F.2d at 989; *Joseph*, 332 F. Supp. 2d at 574 ("[B]oth the Supreme Court and Second Circuit have held that there are situations where the burden of persuasion at a suppression hearing can shift to the Government to prove, by a preponderance of the evidence, that the proffered evidence is valid.") (summarizing cases). "[T]he controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence." *United States v. Matlock*, 415 U.S. 164, 177 n.14 (1974).

B. Whether Law Enforcement Obtained Private Information from Defendants Through a Warrantless Search.

The affidavits state that a law enforcement officer performed an investigation of peer-to-peer file sharing using automated software to determine whether IP addresses in his or her jurisdiction had offered to share files indicative of child pornography. Defendants argue that the software actually has the ability to access private information

which Defendants did not make available for sharing. After a lengthy evidentiary hearing, there is no factual support for this claim. Instead, the evidence overwhelming demonstrates that the only information accessed was made publicly available by the IP address or the software it was using. Accordingly, either intentionally or inadvertently, through the use of peer-to-peer file sharing software, Defendants exposed to the public the information they now claim was private.

The Supreme Court has repeatedly explained that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"). In *Smith*, the government installed at the telephone company's headquarters a "pen register" that recorded the numbers dialed on a certain telephone; the pen register, however, did not record the content of the phone calls. *Smith*, at 736 n.1, 737, 741. The Court concluded there was no legitimate expectation of privacy in the numbers the defendant dialed, reasoning: "First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. "Second, even if [the defendant] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743-44 (internal quotation marks and citations omitted).

The *Smith* Court analogized the facts before it to those at issue in *United States v. Miller*, 425 U.S. 435 (1976), wherein the Court "held that a bank depositor has no 'legitimate expectation of privacy' in financial information 'voluntarily conveyed to banks and exposed to their employees in the ordinary course of business.'" *Smith*, 442 U.S. at 744. (quoting *Miller*, 425 U.S. at 442.) The Court explained "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the

assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. The *Miller* Court's analysis "dictate[d]" the result in *Smith*: "When he used his phone, [the defendant] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [the defendant] assumed the risk that the company would reveal to police the numbers he dialed." *Smith*, 442 U.S. at 744. A similar conclusion is warranted here.

Defendants conveyed certain information to the public when they used peer-to-peer file sharing software and made certain files available for sharing. This includes files that they were in the midst of downloading even if they later intended to maintain those files in a private, non-shared folder when the download was complete. Accordingly, the only question is whether Defendants maintained a reasonable expectation of privacy in the face of public disclosure of that information.

The federal courts of appeals that have examined the privacy implications of searching peer-to-peer networks for files potentially containing child pornography have concluded that a search of publicly available information does not violate a computer user's reasonable expectation of privacy. For example, in *United States v. Borowy*, 595 F.3d 1045 (9th Cir. 2010), the Ninth Circuit rejected the argument that the defendant had a reasonable expectation of privacy in files that were shared on a peer-to-peer file sharing site, even though the defendant intended to maintain the files as private. *See id.* at 1048 ("[Defendant's] subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access."). The *Borowy* court also addressed whether use of a forensic software program, which is not available to the public, renders the search unlawful, and concluded that it did not. *See id.* (describing the software as "function[ing] simply as a sorting mechanism to prevent the government from having to sift, one by one, through [the defendant's] already publically exposed files").[3]

[3] Defendants point out that the *Bowory* court observed that "where the information was not already exposed to the public at large, where the hash-mark analysis might reveal more than

Other circuits have reached similar conclusions. *See United States v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011) (concluding that search of defendant's computer did not constitute an unlawful search because "the contents of the shared folder on [defendant's] computer were knowable to law enforcement without physical intrusion in[to] [defendant's] house because this information was also available to members of the public"); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (concluding that defendant "had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where [defendant] admittedly installed and used Limewire to make his files accessible to others for file sharing"); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (concluding defendant had no expectation of privacy in his subscriber information because "he had peer-to-peer software on his computer, which permitted anyone else on the internet to access at least certain folders in his computer," and "such access could expose his subscriber information to outsiders."). Lower courts have also found that software utilized by law enforcement officers to investigate files shared on peer-to-peer file sharing sites permits "no greater access to other users' shared files than any other Gnutella client." *United States v. Gabel*, 2010 WL 3927697, at *2 (S.D. Fla. Sept. 16, 2010), *adopted*, 2010 WL 3894134 (S.D. Fla. Oct. 4, 2010) (examining ShareazaLE software).

Courts that have specifically considered Peer Spectre have found the evidence it gleans admissible. *See United States v. Willard*, 2010 WL 3784944, at *3 (E.D. Va. Sept. 20, 2010) (denying motion to suppress and ruling Peer Spectre "did not constitute a wiretap because the software does not intercept electronic communications" but instead "reads publicly available advertisements from computers identified as offering images of

---

whether a file is known child pornography, or where the government 'vacuumed' vast quantities of data indiscriminately – we might find a Fourth Amendment violation." *Bowory*, 595 F.3d at 1048 n.2. Defendants argue that their cases are of the type that the *Bowory* court declined to address because law enforcement accessed system files on their computers, and thus recorded information about files that the users expressly decided not to make public. However, there is no evidence that law enforcement accessed any private system files on any of the Defendants' computers. Defendants' legal argument that these cases fall within the *Bowory* exceptions thus lacks a factual basis.

child pornography for distribution and identifies their IP addresses"); *see also United States v. Driver*, 2012 WL 1605975, at *2 (E.D. Mich. May 8, 2012) (explaining results of law enforcement's undercover investigation, noting that Peer Spectre "look[s] for files using known search terms" and captures "IP address, date/time, hash value, [and] filename" of such files, and ruling that this evidence is admissible against a criminal defendant as inextricably intertwined with the charged child pornography offense). Defendants cite no authority for the proposition that they retained a reasonable expectation of privacy in the information obtained by Peer Spectre or any other CPS product.

Because there is no evidence that law enforcement's use of automated software reached information on Defendants' computers that was not made available for sharing by the public, Defendants' motions to suppress on the basis of a warrantless search in violation of the Fourth Amendment must be DENIED.

C. Whether *Franks* Requires Exclusion of Certain Information and Whether, If Excluded, the Search Warrants Lack Probable Cause.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. A magistrate judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "A search warrant affidavit is presumed reliable." *United States v. Klump*, 536 F.3d 113, 119 (2d Cir. 2008). "[T]he task of a reviewing court is simply to ensure that the 'totality of the circumstances' afforded the [issuing judge] 'a substantial basis' for making the requisite probable cause determination." *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (quoting *Gates*, 462 U.S. at 238).

Defendants cite *Franks v. Delaware*, 438 U.S. 154 (1978), in support of their contention that the search warrant affidavits in their respective cases contain deliberately or recklessly false statements or omissions which, if corrected, defeat a finding of

probable cause. To secure a *Franks* hearing, Defendants must make a "'substantial preliminary showing' that a deliberate falsehood or statement made with reckless disregard for the truth was included in the warrant affidavit and the statement was necessary to the judge's finding of probable cause." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008) (quoting *Franks*, 438 U.S. at 155-56, 170-71).

A search warrant affiant "does not *necessarily* act with 'reckless disregard for the truth' simply because he or she omits certain evidence that a reviewing court, in its judgment, considers to be "clearly critical." *United States v. Rajaratnam*, 719 F.3d 139, 154 (2d Cir. 2013). "Rather, the reviewing court must be presented with credible and probative evidence that the omission of information" in the search warrant application "was 'designed to mislead' or was 'made in reckless disregard of whether [it] would mislead.'" *Id.* (alteration in original) (quoting *United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003)). This is a subjective inquiry:

> To prove reckless disregard for the truth, the defendants [must] prove that the affiant in fact entertained serious doubts as to the truth of his allegations. Because states of mind must be proved circumstantially, a factfinder may infer reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations.

Id. (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)).

Information omitted from an affidavit is material only if it affects a finding of probable cause. In other words, a warrant is invalid "*only* if the affidavit as supplemented by the omitted material *could not* have supported the existence of probable cause." *United States v. Lueth*, 807 F.2d 719, 726 (8th Cir. 1986); *see also United States v. Garza*, 980 F.2d 546, 551 (9th Cir. 1992) (refusing to suppress evidence when, "[e]ven if the misstatements were corrected and the omissions supplied, the affidavit would furnish probable cause for issuance of the warrant").

Defendants seek to satisfy their initial burden under *Franks* by pointing to an array of statements in, and omissions from, the search warrant affidavits which they contend are either false or misleading. Many of Defendants' challenges may be dismissed

summarily as they are either unsupported by the facts or have no potential to affect a determination of probable cause.

1. *Franks* Challenges Which Are Not Supported by a False or Misleading Statement Or Omission.

Despite Defendants' arguments to the contrary, law enforcement disclosed to the magistrate judge its use of automated software in conducting its investigations and the information derived therefrom:

> [L]aw enforcement used software that automates the process of searching for computers in Vermont that are suspected of sharing images or videos depicting child pornography on P2P networks. This software is designed to replace the searches that were previously done manually by law enforcement and the public. The software reports information that is discoverable by the general public using publicly available P2P software. Investigators who have access to this software physically activate the software in order to begin the search process which then automatically reads the publicly available advertisements from computers that are sharing files depicting child pornography. The software reads the offers to participate in the sharing of child pornography and logs the IP address, time, date, SHA1 values, and file name of each individual computer in the same way every time. Law enforcement has validated this software by running identical search terms through the manual method described above and have confirmed that the software performs in the same way.

Ex. 7 at ¶ 33; Ex. 8 at ¶ 33; Ex. 9 at ¶ 33. Defendants nonetheless contend that law enforcement should have also disclosed that the automated software generated information which was sent to a third party database which then produced a report that was transmitted to law enforcement for further investigation. Notably absent from Defendants' briefs is any citation to any instance in which suppression was granted on this basis. Defendants are simply incorrect in their further assertion that all of the information set forth in the affidavits was acquired from a third party source and no other investigation was performed. Each affidavit identifies the steps law enforcement took to verify and corroborate the information received from the automated software.

Defendants further contend that law enforcement was obligated to advise the magistrate judge of the names of each of the automated software programs used, how and

from whom they were obtained, and facts about the creation and maintenance of the databases which they accessed. In essence, Defendants assert that if the magistrate judge knew that TLO, a data fusion company based in Boca Raton, Florida, offered automated software programs called Peer Spectre, Lime Scanner, Lime Crawler, ShareazaLE, and Nordic Mule as part of a suite of software called CPS, and generated reports for law enforcement to use in their investigation of child exploitation crimes, the determination of probable cause would somehow be different. This argument is without merit. The material fact that law enforcement was obligated to disclose was that law enforcement automated the process of searching for files indicative of child pornography by using software that reported certain publicly available information. This fact was fully disclosed. More exacting details and disclosures simply were not required to establish probable cause. *See United States v. Martin*, 426 F.3d 83, 86 (2d Cir. 2005) ("[P]robable cause only requires 'the probability, and not a prima facie showing, of criminal activity.'") (quoting *Gates*, 462 U.S. at 235). Moreover, if made, these additional disclosures would not have affected the determination of probable cause because they would have merely provided the magistrate judge with further information regarding the source and identity of the automated software. Defendant Thomas concedes this point.[4]

Defendants next assert that after CPS investigative tools were created and offered for use, either TLO or law enforcement had an obligation to further test them before they could be employed by law enforcement. As a corollary to this argument, Defendants contend that it was insufficient and misleading to advise the magistrate judge that the

---

[4] Counsel for Defendant Thomas: "And my bottom-line point is why would you not tell the magistrate that I'm pulling this information from a data base. . . . The source of that information should have been made known to the magistrate so that he could evaluate it. Am I suggesting that if they told Magistrate Judge Conroy that, gee, this is [a] law enforcement organized venture and law enforcement has done all of this stuff to put together this database and this is the database that I drew from that he wouldn't have granted the affidavit? Probably not. He probably would have."

The Court: But that's a key concession. I mean that's *Franks*.

(Tr. 7/31/13 at 24-25.)

results from Peer Spectre have been compared to the results from manual searches in order to "validate" this investigative tool. Defendants point to no accepted tests or methodology that should and could have been used to further test the reliability of CPS's products and Ms. Loehrs conceded that they do not exist. Although she hypothesizes regarding how she would create an ideal testing environment, she could cite to no court or scientific journal that has endorsed her approach or recognized it as a standard for the industry.

In addition, because automated software products must use the same protocols as the file sharing programs which they investigate, it makes little sense to argue, as Ms. Loehrs does, that "unreliable" protocols developed by the networks which host the file sharing software programs should not be used by automated software. If the same protocols are not used, the automated software would cease to function. In any event, Defendants confuse the test for determining the admissibility of evidence from an expert witness at trial under Fed. R. Evid. 702 with the more flexible and less demanding standard for evidence necessary to establish probable cause. A determination of probable cause simply does not require the level of certainty which Defendants erroneously argue must be shown before CPS investigative tools can be used. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances.").

Defendants' challenge to the reliance on hash values to identify files made available for sharing by a particular IP address is similarly misplaced. Defendants concede, as they must, that files shared with peer-to-peer software programs all use some form of hash value in order to identify a file. Law enforcement plays no role in the type of hash value chosen. Moreover, law enforcement seeking to investigate file sharing involving peer-to-peer file sharing software on a particular network must at least initially rely upon the type of hash value chosen by the network. It is therefore nonsensical to ascribe fault to law enforcement for using a particular type of hash value. The evidence before the court supports a conclusion that hash values provide information regarding a

particular file's contents that is substantially more reliable than a file's name or size.[5] Indeed, it is the most reliable information available. In these cases, law enforcement physically examined the images associated with the identified hash values and concluded that the identified files contained child pornography. Defendants cite to no authority for their claim that hash values are inherently unreliable or that a direct download of the file is necessary to establish probable cause. Courts have routinely found otherwise. *See, e.g.*, *United States v. Cunningham*, 694 F.3d 372, 376 n.3 (3d Cir. 2012) ("'Although it may be possible for two digital files to have hash values that collide, or overlap, it is unlikely that the values of two dissimilar images will do so.'") (quoting *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011)); *United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012) (addressing a challenge to an exhibit showing video clips from a law enforcement database, the court explained that "the SHA-1 values of these videos matched the SHA-1 values of the files offered for distribution from [defendant's] computer. According to the expert, there was a 99.9999% probability that [the exhibit] contained the same video clips that [defendant] possessed. The admission of [the exhibit] . . . was not unfairly prejudicial") (footnote omitted); *United States v. Willard*, 2010 WL 3784944, at *1 n.1 & *5 (E.D. Va. Sept. 20, 2010) (discussing a police database maintained with records of child pornography, the court noted that "[b]y comparing the SHA1 values of two files, investigators can determine whether the files are identical with precision greater than 99.9999 percent certainty" and rejecting request for *Franks* hearing based upon a claim "that the officers making the affidavit made false statements regarding the accuracy of SHA1").

Defendants next contend that the search warrant affidavits failed to disclose the alleged unreliability of an MD4 hash value which they conflate with an MD5 hash value. This argument is based upon the fallacy that law enforcement somehow affirmatively chose to rely on MD4 values in its investigation when more reliable information was

[5] However, as the government points out, the file names at issue here were alone supportive of a finding of probable cause and their corresponding file sizes provided some indicia that they were not devoid of content.

available. Certain file sharing networks, such as the eDonkey network, use MD4 hash values to identify files for sharing and to facilitate rapid downloads. Accordingly, when investigating use of eDonkey networks for child pornography crimes, law enforcement will receive an MD4 hash value for a target file. Law enforcement may then, as here, seek to bolster the MD4 hash value's reliability by attempting to find the file's equivalent SHA1 value. Defendants fail to cite a single case in which a lack of probable cause has been attributed to the use of an MD4 hash value to identify child pornography. Moreover, both Mr. Wiltse and Ms. Loehrs testified that they have never seen an MD4 hash value collide. As a result, additional information regarding the reliability of MD4 values would not have affected a finding of probable cause.

Defendants next argue that it was misleading for law enforcement to describe its investigation as "undercover" when from Defendants' perspective it was not. Detective Eno credibly testified that the investigation was referred to as "undercover" because it was initiated by an undercover operations unit. In this case, probable cause would not be enhanced or diminished by an investigation that was or was not undercover. Defendants do not argue to the contrary. Moreover, each search warrant affidavit provided ample information from which the magistrate judge could make his own informed determination of whether law enforcement's investigation was "undercover."

Finally, Defendants contend that law enforcement failed to sufficiently verify whether a particular IP address was offering to share potential child pornography because law enforcement merely compared the files that were made available for sharing with database images of the same files, instead of attempting a direct download. In addition, Defendants claim the comparison process was inadequately and misleadingly described in the search warrant affidavits. The search warrant affidavits, however, adequately described how law enforcement verified the images in question:

> As part of this operation, Detective Corporal Gerry Eno of the Vermont Internet Crimes Against Children (ICAC) Task Force and the South Burlington Police Department confirmed that each SHA1 value of interest to the investigation actually represents an image or movie that depicts child pornography. Detective Corporal Eno did this by viewing an image or

> movie with the same SHA1 signature as the shared file. Detective Corporal Eno located the image or movie in the VT ICAC database, or otherwise obtained a copy from another source (or multiple sources) on the P2P network.

Ex. 7 at ¶ 32; Ex. 8 at ¶ 32; Ex. 9 at ¶ 32. Defendants fail to demonstrate any aspect of this disclosure which is false or misleading. *See United States v. Adams*, 110 F.3d 31, 33 (8th Cir. 1997) (finding no *Franks* violation when "warrant was based on true information"). They are simply incorrect that the comparison took place by reference to TLO's database because TLO's database contains no images of child pornography. Moreover, they cite no authority for the proposition that a direct download or "active steps" (Case 5:12-cr-37; Doc. 104 at 2) are required before probable cause may be established. Even without a direct download, courts have consistently found probable cause exists when an IP address that appears to have accessed child pornography can be traced to an identifiable residence. *See United States v. Haymond*, 672 F.3d 948, 959 (10th Cir. 2012) (finding that a supporting affidavit, which stated "that [the officer] observed a user with an IP address linked to [defendant's] residence who had numerous files of child pornography available[,]" was sufficient to establish probable cause); *Stults*, 575 F.3d at 843-44 (concluding that the affidavit, which, among other things, "stated that an IP address traced to [defendant] was identified as accessing child pornography sites[,]" created probable cause to search defendant's residence); *United States v. Perez*, 484 F.3d 735, 740-42 (5th Cir. 2007) (finding probable cause that evidence would be found at the physical address associated with the IP address from which child pornography was transmitted). Here, each affidavit established the requisite nexus.

None of the foregoing challenges satisfies Defendants' initial burden under *Franks*, and the court therefore does not address them further.

2. Further Analysis of Three of Defendants' *Franks* Challenges.

Only three of Defendants' *Franks* challenges merit further analysis, and they do so only because Defendants have identified three statements in the search warrant affidavits which are inaccurate. First, Defendants point out that each of the affidavits recites in a single sentence that a particular IP address *shared* certain files suspected to be child

pornography. Ex. 7 at ¶ 35; Ex. 8 at ¶ 35; Ex. 9 at ¶ 34. Law enforcement concedes that this statement should be corrected to reflect that the IP address *offered to share* certain files - a term used elsewhere in the affidavits. *See* Ex. 7 at ¶ 34; Ex. 8 at ¶ 34; Ex. 9 at ¶ 34. While this difference may be material in determining whether a distribution rather than a possession charge is supported by the evidence, it does not affect the determination of probable cause. Whether a potential child pornography file is "offered to share" or actually "shared," an IP address advertising that file is likely to be associated with a computer that contains child pornography. Accordingly, if corrected to reflect the proper terminology, the probable cause determination would remain unchanged. Moreover, there is no evidence that law enforcement used the term "shared" instead of "offered to share" in order to intentionally or recklessly mislead the magistrate judge.

Second, the search warrant affidavits erroneously state that an MD4 hash value may be "converted" into a SHA1 value. The use of the term "converted" is inaccurate because no "conversion" actually takes place. Instead, a law enforcement officer accesses a database maintained by TLO, or one that is publicly available, to determine the corresponding SHA1 value attributed to a file bearing an MD4 hash value. This correction to the search warrant affidavits would also have no impact of an analysis of probable cause because it would only more accurately explain how law enforcement attempted to buttress the reliability of the MD4 hash value by finding its SHA1 equivalent.

Defendant Thomas makes a more specific argument by pointing out that two of the files identified in the search warrant affidavit related to his residence were allegedly advertised on the eDonkey system, which does not utilize SHA1 values. The affidavit in support of the search warrant explains that law enforcement "can hash the file using the SHA1 digital algorithm and determine its SHA1 value" (Ex. 7 at ¶ 29) and that "law enforcement needs to convert the eDonkey hash value to SHA1 because it is able to search for files by hash value only on the Gnutella network." *Id.* Defendant Thomas argues that the government has failed to adequately explain how law enforcement may hash a file using the SHA1 algorithm if the file is not downloaded. Defendant Thomas

contends that this left the magistrate judge with "a distorted and inaccurate picture." (Case 5:12-cr-37; Doc. 47 at 10.)

Defendant Thomas is correct that a file cannot be "hashed" if it is not in the law enforcement officer's physical possession. The government, however, persuasively counters that it was not necessary to describe in the affidavit how a file is hashed and how an eDonkey hash value may be cross-referenced with its corresponding SHA1 value for the same file because these facts are "minute technological detail." (Case 5:12-cr-37; Doc. 62 at 12.) The court agrees. Although the search warrant affidavit fails to accurately describe the process for hashing a file and finding a SHA1 value for an MD4 file, in the absence of any evidence that cross-referencing is either technologically unfeasible or was not reliably performed, the additional information would contribute little to a probable cause analysis, beyond ascribing the correct terminology for the cross-referencing process.

Third, the affidavits state that partially downloaded files will not be shown as available for sharing:

> If the sharing computer is in the process of downloading file(s) (incomplete files), these files do not appear in the list. Only those [files] that are completely downloaded and being shared will be displayed in this list.

Ex. 7 at ¶ 23; Ex. 8 at ¶ 23; Ex. 9 at ¶ 23. Each expert witness testified that incomplete files may be made available for sharing in at least three ways. First, a query may reach a computer in the process of downloading a file that contains a responsive term and generate a query hit message that the file is available for sharing accompanied by the hash value the file will bear upon completion of the download. This may occur even if the file is not actually available for sharing until the download is complete and even if the file is later moved to a non-shared folder. Second, the default settings of a particular version of peer-to-peer file sharing software or a user may designate partial or incomplete files as available for sharing. And third, a user may, as Ms. Loehrs did, manually place incomplete, deleted, or corrupted files in a shared folder and thereby make them available for sharing. If the affidavits were corrected to reflect this information, Defendants do not

explain how the probable cause determination would be affected. At best, it makes it only slightly less likely that child pornography will be found on a computer offering to share the file. As the court in *Moran* concluded, this does not defeat a finding of probable cause.

3. Subjective Intent to Deceive or Mislead.

With regard to each of Defendants' *Franks* challenges, there was no accompanying evidence of any intentional or reckless subjective intent to deceive or mislead the magistrate judge. To the contrary, there is ample evidence of subjective and objective good faith and reasonableness. The affiants, none of whom is a computer forensic expert, engaged in a careful and time-consuming collaborative process in order to describe at length in their respective search warrant affidavits the information yielded by their investigation and why they believed it supported a finding of probable cause. They then sought and obtained an Assistant U.S. Attorney's approval of their warrant applications. The incorrect statements Defendants have identified are only minor details among a wealth of information contained in the search warrant affidavits which demonstrated probable cause and which supported the issuance of the warrants. *See United States v. Arvizu*, 534 U.S. 266, 274 (2002) (holding that "evaluation and rejection of seven of the [officer's observations] in isolation from each other does not take into account the totality of the circumstances, as our cases have understood that phrase") (internal quotation marks omitted).

"[T]he ultimate inquiry is whether, after putting aside erroneous information and correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause." *Rajaratnam*, 719 F.3d at 146 (internal quotation marks or alterations omitted). Here, that standard is easily met. Moreover, in the absence of "credible and probative evidence that the . . . information . . . was designed to mislead or was made in reckless disregard of whether it would mislead," *id.* at 154 (internal quotations marks and alterations omitted), suppression is not warranted.

D. Good Faith Exception.

As the government points out, even if the court found that the search warrants in these cases lacked probable cause, suppression would not be warranted if law enforcement relied upon the warrants in good faith. "As the Supreme Court recently reminded courts, suppression is 'our last resort, not our first impulse' in dealing with violations of the Fourth Amendment." *Clark*, 638 F.3d at 99 (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)). Accordingly, "the exclusionary rule barring illegally obtained evidence from the courtroom does not apply to evidence seized 'in objectively reasonable reliance on' a warrant issued by a detached and neutral . . . judge, even where the warrant is subsequently deemed invalid." *Falso*, 544 F.3d at 125 (quoting *United States v. Leon*, 468 U.S. 897, 922 (1984)). Here, the good faith exception would apply.

CONCLUSION

For the foregoing reasons, Defendants' Motions to Suppress are hereby DENIED. SO ORDERED.

Dated at Rutland, in the District of Vermont, this 8th day of November, 2013.

/s/ ***Christina Reiss***

Christina Reiss, Chief Judge
United States District Court